(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－237249

(43)公開日　平成６年(1994)８月23日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ 9/06					
9/14					
9/22					
		7117－5K	Ｈ０４Ｌ 9/02		Ｚ
		7117－5K	9/04		

審査請求　未請求　請求項の数３　ＯＬ　（全　８　頁）　最終頁に続く

(21)出願番号　特願平5－122326

(22)出願日　平成５年(1993)５月25日

(31)優先権主張番号　特願平4－338466

(32)優先日　平４(1992)12月18日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001258
川崎製鉄株式会社
兵庫県神戸市中央区北本町通１丁目１番28号

(72)発明者　髙橋　利夫
東京都千代田区内幸町二丁目２番３号　川崎製鉄株式会社東京本社内

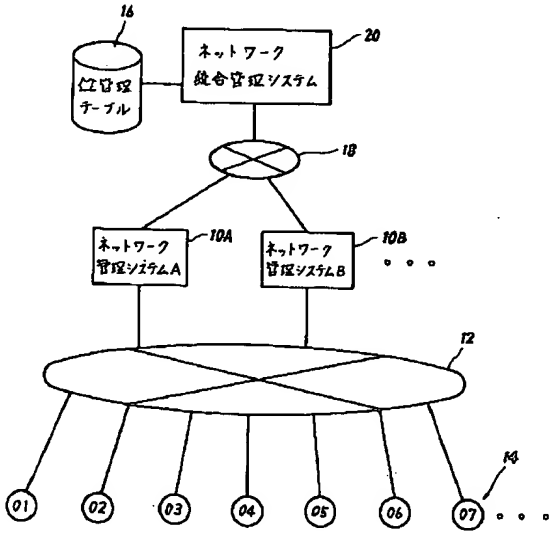
(74)代理人　弁理士　髙矢　諭　（外２名）

(54)【発明の名称】　ネットワーク管理のセキュリティシステム

(57)【要約】

【目的】　ネットワーク管理を行うためのデータ通信に対する第３者による妨害を確実に防止する。

【構成】　ネットワーク管理システム１０から通信回線１２を介して下位の管理対象１４や上位のネットワーク統合管理システム２０との間でデータ通信を行う際、鍵管理テーブル１６に格納されている、ネットワーク管理システム１０と該当管理対象１４との間の通信に使用する鍵を、両者間のデータ通信の回数をカウントアップし、その回数が所定の基準回数（保存期間）に達した時点で、その鍵を新たに更新する。その際、該当管理対象に対する鍵の更新は、管理システムで新たなる鍵を旧い鍵で暗号化し、それをデータ通信として管理対象に伝送して行う。



1

【特許請求の範囲】

【請求項１】ネットワークを構成する装置を管理対象として、ネットワーク管理システムで管理するネットワーク管理のセキュリティシステムにおいて、

ネットワーク管理システム側に、各管理対象との通信に使用する鍵を格納する鍵管理手段と、新たな鍵を生成する手段と、管理対象毎に通信データを鍵で暗号化して伝送する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認証する手段とを備えると共に、

各管理対象毎に、新たな鍵に更新する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認証する手段とを備えていることを特徴とするネットワーク管理のセキュリティシステム。

【請求項２】請求項１において、

鍵を、各管理対象毎に定期的に更新する手段を備えていることを特徴とするネットワーク管理のセキュリティシステム。

【請求項３】大規模ネットワークを構成する複数のネットワーク管理システムを管理対象として、ネットワーク統合管理システムで管理するネットワーク管理のセキュリティシステムにおいて、

ネットワーク統合管理システム側に、各ネットワーク管理システムとの通信に使用する鍵を格納する鍵管理手段と、新たな鍵を生成する手段と、ネットワーク管理システム毎に通信データを鍵で暗号化して伝送する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認識する手段とを備え、

各ネットワーク管理システム毎に、新たな鍵に更新する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認識する手段とを備えると共に、

鍵を各ネットワーク管理システム毎に定期的に更新する手段を備えていることを特徴とするネットワーク管理のセキュリティシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ネットワーク管理のセキュリティシステム、特に第１種及び第２種電気通信事業者等が運営する広域且つ大規模なネットワーク等を管理するネットワーク管理システムに適用して好適な、ネットワーク管理のセキュリティシステムに関する。

【０００２】

【従来の技術】ネットワークを構成する各種装置を管理対象とするネットワーク管理システム、又は、広域且つ大規模なネットワークを管理するのに、そのネットワーク構成要素を地理的又は論理的に分割して、その区分内の構成要素だけを管理するネットワーク管理システム

2

と、それら複数のネットワーク管理システムを統合管理するネットワーク管理システムが知られている。このネットワーク管理システムが管理対象とする各種装置としては、交換機、伝送装置、多重化装置、中継装置、分岐装置等がある。

【０００３】上記ネットワーク管理システムは、上記各種管理対象についての論理的、物理的な構成状態の制御、スループットや履歴情報を含む誤り率の制御・解析、異常動作の検出・切り離し制御、管理対象の使用に関するデータの収集や処理、管理対象に対するアクセスの制御等を１つの処理装置で集中的に処理する機能を有している。

【０００４】上記ネットワーク管理システムでは、該システムと管理対象との間で行われる管理処理に必要な管理情報や命令に関するデータ通信に、第三者が侵入してデータの盗聴や改ざんを行い、管理対象の正常な動作を妨害することがある。

【０００５】

【発明が解決しようとする課題】しかしながら、従来のネットワーク管理システムとしては、ネットワークを構成する管理対象へのアクセスを制御するだけで、ネットワーク管理を行うためのデータ通信に対する妨害からネットワークを防御する技術はほとんど考えられていなかった。

【０００６】その理由は、広域ネットワークを集中的に管理するシステムがまだ十分に実用段階まで到っていなかったこと、ネットワーク管理用データ通信に対する妨害への認識が少なかったこと、通信データの暗号化に関る鍵の管理が非常に困難だったことにある。

【０００７】本発明は、前記従来の問題点を解決するべくなされたもので、ほぼ実用段階に入った広域ネットワークの集中管理システムを運用する上で新たな問題となっている、ネットワーク管理用データ通信に対する第３者の侵入による管理情報や命令情報の盗聴や改ざんから通信データを防御するために、通信データを暗号化する際に必要となる鍵を容易に管理することができる、ネットワーク管理のセキュリティシステムを提供することを課題とする。

【０００８】

【課題を解決するための手段】本発明は、ネットワークを構成する各装置を管理対象として、ネットワーク管理システムで管理するネットワーク管理のセキュリティシステムにおいて、ネットワーク管理システム側に、各管理対象との通信に使用する鍵を格納する鍵管理手段と、新たな鍵を生成する手段と、管理対象毎に通信データを鍵で暗号化して伝送する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認証する手段とを備えると共に、各管理対象毎に、新たな鍵に更新する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信

データが正当であることを認証する手段とを備えた構成とすることにより、前記課題を達成したものである。

【０００９】本発明は、前記ネットワーク管理のセキュリティシステムにおいて、鍵を、各管理対象毎に定期的に更新する手段を備えたことにより、前記課題を一層確実に達成したものである。

【００１０】本発明は、又、大規模ネットワークを構成する複数のネットワーク管理システムを管理対象として、ネットワーク統合管理システムで管理するネットワーク管理のセキュリティシステムにおいて、ネットワーク統合管理システム側に、各ネットワーク管理システムとの通信に使用する鍵を格納する鍵管理手段と、新たな鍵を生成する手段と、ネットワーク管理システム毎に通信データを鍵で暗号化して伝送する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認識する手段とを備え、各ネットワーク管理システム毎に、新たな鍵に更新する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認識する手段とを備えると共に、鍵を各ネットワーク管理システム毎に定期的に更新する手段を備えたことにより、同様に前記課題を達成したものである。

【００１１】

【作用】本発明においては、ネットワーク管理システムやネットワーク統合管理システム側に、各管理対象（ネットワーク統合管理システムの場合にはネットワーク管理システム）との通信に使用する鍵を格納する鍵管理手段と、新たな鍵を生成する手段と、通信データを鍵で暗号化して伝送する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認証する手段とを備えると共に、各管理対象毎に、新たな鍵に更新する手段と、暗号化された通信データを鍵により復元する手段と、復元された通信データが正当であることを認証する手段とを備えたので、ネットワーク管理システムやネットワーク統合管理システムでは、例えば予め定めた通信回数毎に新たな鍵を生成し、格納すると共に、それを通信データとして暗号化して該当する管理対象に伝送することにより、該当管理対象では、そのデータを旧い鍵で復元し、それを新たな鍵として更新することが可能となるため、通信データを鍵で暗号化して伝送する通信を、ネットワーク管理システムやネットワーク統合管理システムと管理対象との間で繰り返しながら、データの暗号化・復元に使用する鍵の更新を定期的に行うことが可能となる。

【００１２】このように、本発明では、鍵の管理及び更新を、ネットワーク管理システムと該当管理対象との間のデータ通信そのものを利用して行うので、管理用データ通信を、簡単にしかも確実に第３者による妨害から防ぐことが可能となる。

【００１３】この鍵の管理・更新に使用するデータ通信

としては、管理システムの要求命令に対して管理対象が行う管理情報の送信、管理システムが管理対象に対して行う管理データの送信や動作指示命令の送信、管理対象から管理システムに通知する異常状態の送信等がある。

【００１４】

【実施例】以下、図面を参照して、本発明の実施例を詳細に説明する。

【００１５】図１は、ネットワーク管理システムと、下位の管理対象の間に本発明を適用した、本発明に係る第１実施例のネットワーク管理のセキュリティシステムにより管理する、モデル化したネットワークを示す線図である。

【００１６】図中、符号１０は、ネットワーク管理システムであり、該当ネットワーク管理システム１０によりネットワーク１２を介して接続されている管理対象１４（図では、０１、０２の識別番号で２つだけ示してある）が管理されるようになっている。

【００１７】上記管理対象１４としては、前述した如く、ネットワークを構成する交換機、伝送装置、多重化装置、中継装置、分岐装置等がある。

【００１８】本実施例では、上記ネットワーク管理システム１０に鍵管理テーブル１６が組み込まれており、この鍵管理テーブル１６では、図２に示すように、管理対象毎の鍵、鍵の保存期間、及び管理対象との通信回数が格納されている。

【００１９】上記ネットワーク管理システム１０は、新たな鍵を生成し、格納すると共に、それを通信データ（新たな鍵を含む）を暗号化して該当する管理対象に伝送する機能と、各管理対象から伝送されてくる暗号化された通信データを鍵により復元し、その復元された通信データが正当であることを認証する機能をも有している。

【００２０】又、各管理対象は、旧い鍵をネットワーク管理システム１０から伝送される新たな鍵に更新すると共に、通信データ（新たな鍵を含む）を鍵により復元し、復元された通信データが正当であることを認証する機能と、ネットワーク管理システムに対して通信データを暗号化して伝送する機能とを有している。

【００２１】次に、本実施例の作用を、図３、図４のフローチャートを用いて説明する。

【００２２】図３は、ネットワーク管理システム側で実行される処理手順を示したフローチャートであり、図４は、管理対象側で実行される処理手順を示したフローチャートである。なお、これらフローチャートでは、理解し易いようにネットワーク管理システムでは３００番代、管理対象では４００番代の番号で処理ステップをそれぞれ示した。

【００２３】上記ネットワーク管理システム１０と管理対象１４との間でデータ通信が発生すると、ネットワーク管理システム１０では、鍵管理テーブル１６の該当す

る管理対象について通信回数をカウントアップする（ステップ３０１）。

【００２４】次いで、カウントアップした通信回数と、該当管理対象の通信回数として設定されている保存期間とを比較し（ステップ３０２）、両者が等しくなったならば鍵の更新を行う。この鍵の更新は、まず、通信回数をゼロクリアし（ステップ３０３）、次いで新しい鍵を生成し（ステップ３０４）、それを暗号化して該当管理対象に通信データとして送信する（ステップ３０５、３０６）。

【００２５】上記の如く、ネットワーク管理システム１０から暗号化された新しい鍵が該当管理対象に送信されると、ここでは図４のフローチャートに示すように、ステップ４０１で通信タイプが鍵更新側に切替わり、鍵更新に関するデータを受信し（ステップ４０７）、それまで使用していた旧い鍵により新しい鍵に関するデータを復元し（ステップ４０８）、正当なデータか否かを判定すると共に、正常である場合には認証してそれを新しい鍵として更新する（ステップ４０９、４１０）。

【００２６】又、ネットワーク管理システム１０側では、前記ステップ３０６で、該当管理対象に対して新しい鍵のデータを送信した後、鍵管理テーブル１６に格納されている該当管理対象の旧い鍵を、新たに生成した新しい鍵に更新し、設定し直す（ステップ３０７）。

【００２７】以上のように、ネットワーク管理システム１０の鍵管理テーブル１６に格納されている該当管理対象の鍵と、該当管理対象における鍵とを新しく設定し直した後、ステップ３０８で通信タイプが送信になっている場合には、任意の通信データを、更新後の該当管理対象の鍵により暗号化し（ステップ３０９）、該当管理対象に送信する（ステップ３１０）。

【００２８】前記ステップ３１０でネットワーク管理システム１０側から暗号化された通信データが送信されると、該当管理対象では、ステップ４０１で通信タイプが受信側に切替わり、そのデータを受信して（ステップ４０４）、該当管理対象自身で保存している鍵によりデータの復元を行い（ステップ４０５）、正当なデータであるか否かを判定し、正しい場合にはそれを認証する（ステップ４０６）。

【００２９】一方、該当管理対象から通信データの送信を行う場合は、ステップ４０１で通信タイプが送信側に切替わり、該当管理対象自体で保存している鍵によりデータの暗号化を行い（ステップ４０２）、暗号化されたデータをネットワーク管理システム１０へ送信する（ステップ４０３）。

【００３０】上記ステップ４０３で、管理対象側からネットワーク管理システム１０に暗号化された上記データが送信されると、該システム１０側ではステップ３０８で通信タイプが受信側に切替わり、該当データを受信する（ステップ３１１）。このデータを受信すると、鍵管理テーブル１６の該当管理対象の鍵により暗号化されている上記データの復元を行い（ステップ３１２）、正当なデータか否かを判定し、正しい場合にはそれを認証する（ステップ３１３）。

【００３１】以上の処理手順に従って、ネットワーク管理システム１０と管理対象１４との間で通信データの送受信を繰り返すことにより、予め設定されている各管理対象毎の保存期間（通信回数）に応じて、各管理対象との間の通信に使用する鍵が定期的に更新されるため、簡単にしかも確実に暗号化のための鍵の管理を行うことが可能となる。

【００３２】又、図５は、ネットワーク管理システムと、上位のネットワーク統合管理システムの間に本発明を適用した、本発明に係る第２実施例のネットワーク統合管理のセキュリティシステムにより管理する、モデル化したネットワークを示す線図である。

【００３３】図５中、符号２０は、ネットワーク統合管理システムであり、該当するネットワーク統合管理システム２０により、ネットワーク１８を介して接続されているネットワーク管理システム１０A及び１０B等（図では、ネットワーク管理システムA、ネットワーク管理システムBの名称で２つだけ示してある）が統合管理されるようになっている。

【００３４】第２実施例では、上記ネットワーク統合管理システム２０に鍵管理テーブル１６が組み込まれており、第１実施例と同じように、この鍵管理テーブル１６では、図２に示すように、ネットワーク管理システム毎の鍵、鍵の保存期間、及びネットワーク管理システムとの通信回数が格納されている。

【００３５】上記ネットワーク統合管理システム２０は、新たな鍵を生成し、格納すると共に、それを通信データ（新たな鍵を含む）を暗号化して該当するネットワーク管理システムに伝送する機能と各ネットワーク管理システムから伝送されてくる暗号化された通信データが正当であることを認証する機能をも有している。

【００３６】又、各ネットワーク管理システムは、旧い鍵をネットワーク統合管理システム２０から伝送される新たな鍵に更新すると共に通信データ（新たな鍵を含む）を鍵により復元し、復元された通信データが正当であることを認証する機能と、ネットワーク統合管理システム２０に対して通信データを暗号化して伝送する機能とを有している。

【００３７】又、第２実施例の作用は、第１実施例と同様であり、図３、図４のフローチャートによって表され、ネットワーク統合管理システム２０とネットワーク管理システム１０との間で通信データの送受信を繰返すことにより、予め設定されている各ネットワーク管理システムの保存期間（通信回数）に応じて、各ネットワーク管理システムとの間の通信に使用する鍵が定期的に更新されるため、簡単にしかも確実に暗号化のための鍵の

7

管理を行うことが可能となる。

【００３８】以上詳述した本実施例によれば、ネットワーク管理システム１０と管理対象１４との間のあるいは、ネットワーク統合管理システム２０とネットワーク管理システム１０Ａ、１０Ｂとの間の通信に使用する暗号用の鍵を定期的に更新することができるため、簡単ではあるが確実に鍵の管理が行えるようになり、結果としてネットワークの管理のセキュリティを向上することができる。なお、鍵管理テーブルにおける鍵の保存期間の設定は、該当管理対象へのアクセス頻度や、ネットワーク運営上の重要性から適正な値を設定することにより、適切な通信負荷及びセキュリティを維持することができる。

【００３９】以上、本発明について具体的に説明したが、本発明は、前記実施例に示したものに限られるものでなく、その要旨を逸脱しない範囲で種々変更可能である。

【００４０】例えば、前記実施例では、鍵の更新を、予め各管理対象毎に設定されている通信回数に基づいて行う場合を示したが、これに限られるものでなく、保存期間を時間で設定してもよい。

【００４１】

【発明の効果】以上説明した通り、本発明によれば、ネットワーク管理システムにおいて、管理用データ通信に対する第３者の侵入による管理情報や命令情報の盗聴や改ざんから通信データを防御するために、通信データを暗号化する際に必要となる鍵を容易に管理することができる。

8

【図面の簡単な説明】

【図１】本発明に係る第１実施例のネットワーク管理のセキュリティシステムをモデル化して示す説明図

【図２】上記セキュリティシステムが備える鍵管理テーブルを概念的に示す図表

【図３】ネットワーク管理システム側で実行される処理手順を示すフローチャート

【図４】管理対象側で実行される処理手順を示すフローチャート

【図５】本発明に係る第２実施例のネットワーク統合管理のセキュリティシステムをモデル化して示す説明図

【符号の説明】

１０…ネットワーク管理システム

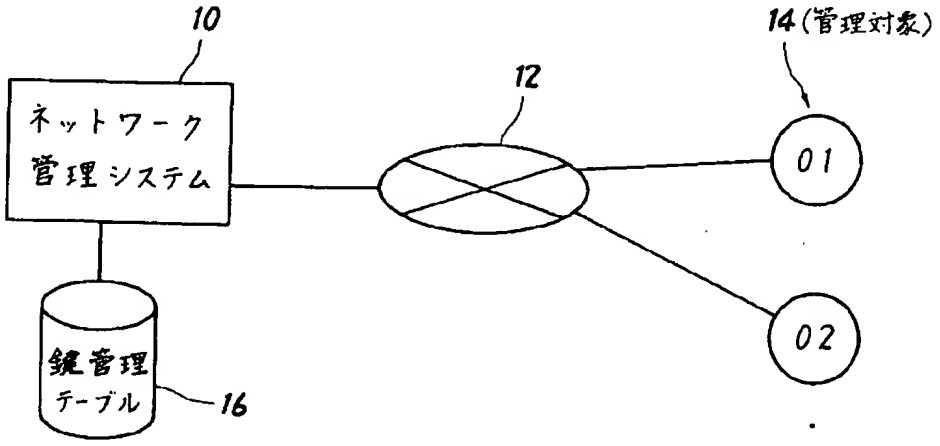
１２、１８…ネットワーク

１４…管理対象

１６…鍵管理テーブル

２０…ネットワーク統合管理システム

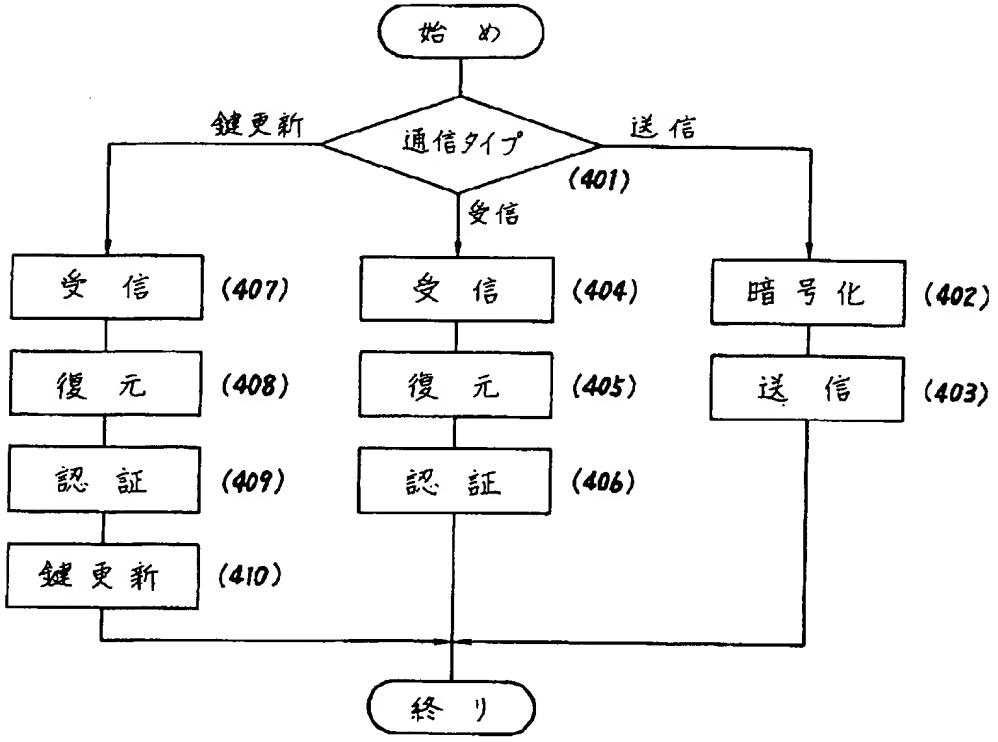
【図１】



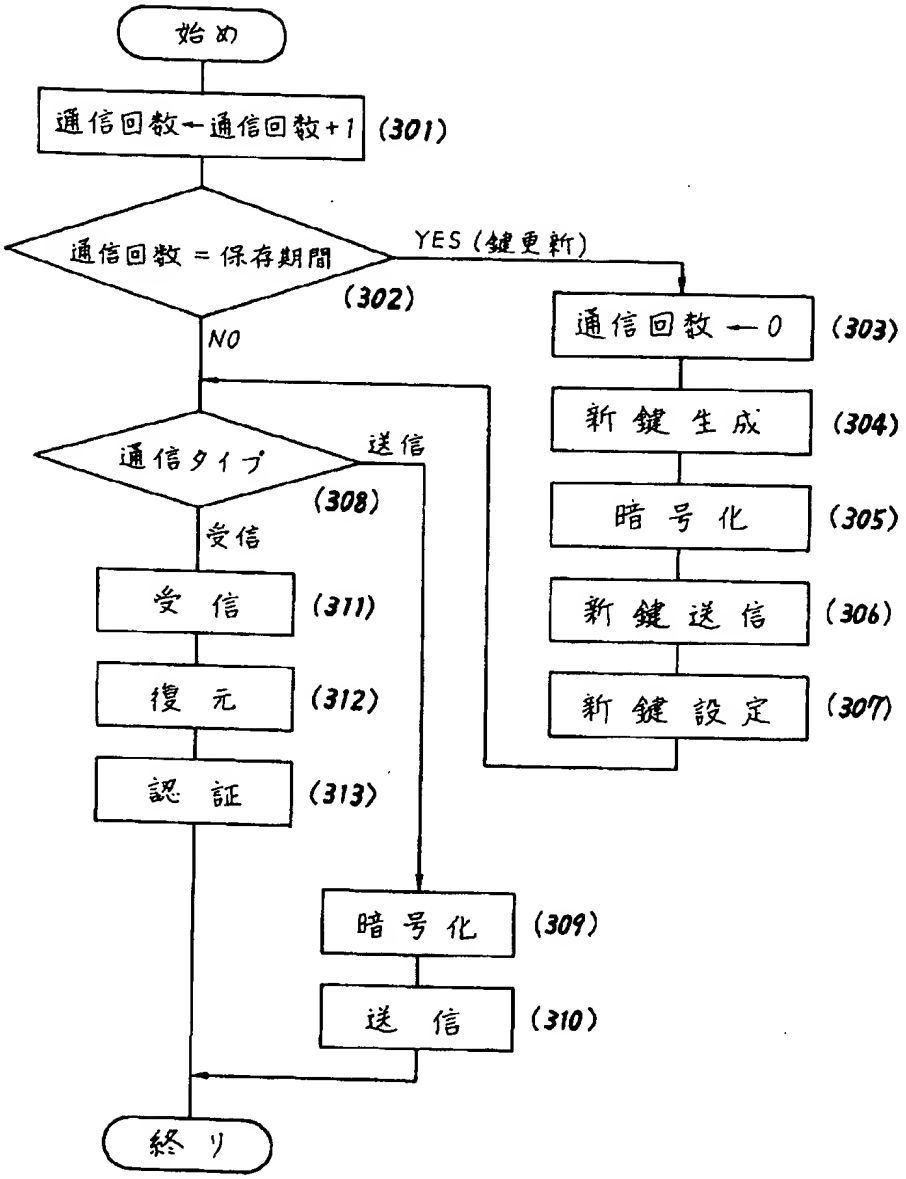
【図2】

管理対象識別番号	鍵	保存期間	通信回数
01	鍵01	40	20
02	鍵02	30	29
⋮	⋮		

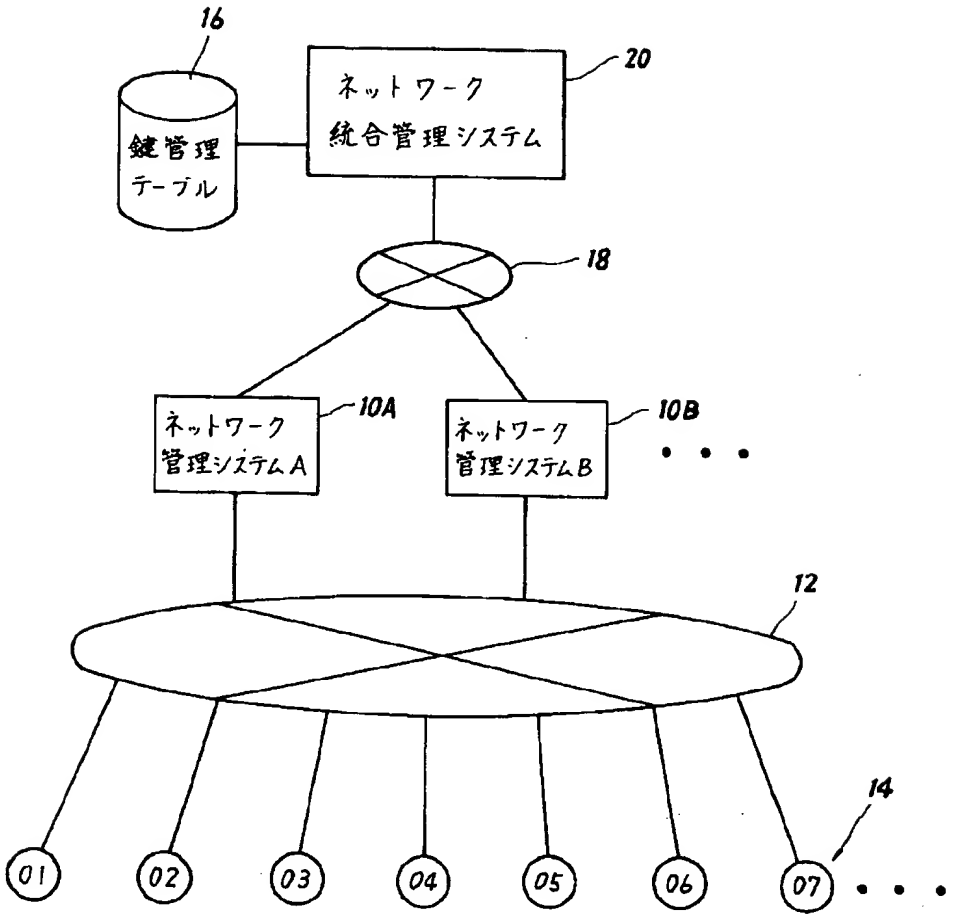
【図4】



【図3】


始め
通信回数←通信回数+1
(301)
通信回数＝保存期間
(302)
YES (鍵更新)
NO
通信回数←0
(303)
新鍵生成
(304)
暗号化
(305)
新鍵送信
(306)
新鍵設定
(307)
通信タイプ
(308)
送信
受信
受信
(311)
復元
(312)
認証
(313)
暗号化
(309)
送信
(310)
終り

【図5】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
H04L 12/24				
12/26				
		8732－5K	H04L 11/08	